**Listing of Claims:**

1. (Previously Presented) A method for detecting an undesirable condition within a messaging network, comprising:

receiving a message from a source;

incrementing a source counter and updating an array of timestamps with a new entry corresponding to a time at which the message from the source was received, the array of timestamps including a timestamp entry for respective source counter increments;

removing entries in the array of timestamps that are older than a fixed window size, and decrementing the source counter for each entry so removed;

comparing the source counter to a source threshold; and

when the source counter exceeds the source threshold, triggering an alarm indicative of an undesirable condition.

2. (Previously Presented) The method of claim 1, further comprising:

identifying a destination for the message;

incrementing a destination counter; and

comparing the destination counter to a destination threshold; and when the destination counter exceeds the destination threshold, triggering a destination alarm.

3. (Original) The method of claim 2, wherein the source threshold and the destination threshold comprise different values.

4. (Previously Presented) The method of claim 1, wherein the message is a short message service message.

5. (Original) The method of claim 1, wherein the messaging network allows for number portability.

6. (Original) The method of claim 1, wherein the messaging network comprises a wireless network.

7. (Original) The method of claim 1, wherein the source comprises a network user and the destination comprises an intermediary vendor.

8. (Previously Presented) A method for detecting a spam event in a messaging network, comprising:

monitoring message traffic in the messaging network;

for a source address associated with a message, creating an entry in a database, setting a source address counter for that source address to a predetermined number and storing a timestamp array including a time at which the message was received, and incrementing the source counter when the source address is again detected and updating the timestamp array with a new timestamp entry corresponding to at time at which the source address was again detected;

removing entries in the timestamp array that are older than a fixed window size, and decrementing the source counter for each entry so removed; and

comparing the source counter for a given source address to a source threshold; and

when the source counter exceeds the source threshold, triggering an alarm indicative of a spam event.

9. (Previously Presented) The method of claim 8, wherein the message traffic comprises short message service messages.

10. (Original) The method of claim 8, wherein the messaging network comprises a wireless network.

11. (Previously Presented) The method of claim 8, wherein the method is performed by an intermediary logically located between two telecommunication service providers.

12. (Previously Presented) A method of detecting a routing loop in a telecommunications network, comprising:

monitoring message traffic passing through an intermediary interconnecting at least two telecommunication service providers;

as message traffic passes through the intermediary, setting a source address counter to a predetermined number and storing a timestamp corresponding to a time at which a first message passed through the intermediary, incrementing the source address counter and adding a new timestamp to an array of timestamps each time the first message passes through the intermediary;

as message traffic passes through the intermediary, setting a destination address counter to a predetermined number and storing a timestamp corresponding to a time at which a second message passed through the intermediary, incrementing the destination address counter and adding a new timestamp to another array of timestamps each time the second message passes through the intermediary;

comparing the source address counter and destination address counter for a given source address and a given destination address, respectively to a source address threshold and destination address threshold; and

when the source address counter and destination address counter, respectively exceed the source address threshold and destination address threshold over the course of a predetermined amount of time, triggering an alarm indicative of a routing loop.

13. (Original) The method of claim 12, wherein the source address threshold and the destination address threshold comprise different values.

14. (Previously Presented) The method of claim 12, wherein the message traffic comprises short message service (SMS) messages.

15. (Original) The method of claim 12, wherein the method detects routing loops caused by number portability.

16. (Original) The method of claim 12, wherein the telecommunications network comprises a wireless network.